

12/4



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/759,127 | 01/12/2001 | Klaus Kursawe | CH919990046-US1 | 9909 |

7590 12/09/2004
Anne Vachon Dougherty
3173 Cedar Road
Yorktown Heights, NY 10598

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT PAPER NUMBER

2131

DATE MAILED: 12/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/759,127

Applicant(s)

KURSAWE ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1,3,5,7,9,11,13-19 and 21-23 is/are allowed.
- 6) ☒ Claim(s) 2,4,6,8,10,12, and 20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in the European Patent Office on January 14, 2000. It is noted, however, that applicant has not filed a certified copy of the foreign application 00100723.6 as required by 35 U.S.C. 119(b).

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 2,4,6,8,10,12, and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Feldman et al, entitled "Optimal Algorithms for Byzantine Agreement".

As per claims 2 and 20, it is disclosed by Feldman et al of a method and computer program product comprising program code means for performing the method for achieving agreement among n participating network devices to a first or second agree-value in an asynchronous network, the agreement arising out of a series of messages being sent and received with a signature by each participating network device. The number t of faulty devices is less than $n/3$. All participating network devices are broadcasted a pre-vote value. A main-vote is performed to amplify

Art Unit: 2131

majorities if $n-t$ pre-vote values are validly received, and broadcasting a main-vote value to all participating network devices. It is decided for a first or second agree-value that is based on the main-vote values and broadcasting to all participating network devices a share-value to open a cryptographic common coin. Share-values are received and assembled, and out of those, a common value wherein a bit is uncovered out of the common value. The step of using the bit as the pre-vote value if the pre-vote values were different is repeated (page 148, abstract ; page 148 section 1.1 through page 150, section 1.2; page 151, section 3.1; page 156, section 4.3 through page 159, section 4.4).

As per claim 4, Feldman et al discloses of the use of a transaction ID (TID)(page 156, section 4.3).

As per claim 6, it is taught by Feldman et al of the usage of threshold signatures (page 149, section 1.2 & page 151, section 3.1).

As per claim 8, Feldman et al teaches of a two threshold coin is used, where t is the maximum number of traitors in the asynchronous network and k , with $n > k > t$, the number of participating network devices needed to obtain the two threshold coin (page 151, section 3.1 & page 158, section 4.4).

As per claim 10, Feldman et al discloses of the number t of faulty devices is larger than $n/3$ if all or part of the faulty devices fail by crashing (page 148, abstract; page 150, section 1.3; & page 151, section 3.1).

As per claim 12, the teachings of Feldman et al recite that $t + 1$ participating devices are used as asynchronous relay stations (page 148, abstract, section 1.1).

Allowable Subject Matter

4. Claims 1,3,5,7,9,11,13-19 and 21-23 are allowed.
5. The following is a statement of reasons for the indication of allowable subject matter:

It was not found to be taught in the prior art of broadcasting a share value to participating network devices to generate an unpredictable bit, receiving k share values from the participating network devices, where k is larger than t , assembling out of those a common value and a deriving bit.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Please see attached PTO-892

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

an

December 7, 2004

Christopher Revak

AU 2131

CR

12/7/04